ENSEMBLE

EUROPEAN COMMISSION

HORIZON 2020

H2020-ART-2016-2017/H2020-ART-2017-Two-Stages

GA No. 769115

ENSEMBLE

ENabling **S**af**E** **M**ulti-**B**rand p**L**atooning for **E**urope

Deliverable No.	D 2.10
Deliverable Title	Iterative process document and Item Definition
Dissemination level	Public

Written By	Prashanth Dhurjati, IDIADA	21-09-2018
	Luca Mengani, IDIADA	
Checked by	Alessandro Coda, CLEPA	27-09-2018
Approved by	Marika Hoedemaeker, TNO	27-09-2018
Status	Final, approved by EC	27-09-2018

Please refer to this document as:

Dhurjati, P., Mengani, L. (2018). *Iterative process document and Item Definition .* D2.10 of H2020 project ENSEMBLE, (www.platooningensemble.eu)

Disclaimer:

ENSEMBLE is co-funded by the European Commission, DG Research and Innovation, in the HORIZON 2020 Programme. The contents of this publication is the sole responsibility of the project partners involved in the present activity and do not necessarily represent the view of the European Commission and its services nor of any of the other consortium partners.

Revision history

Version	Date	Author	Summary of changes	Status
0.1	19/09/2018	Prashanth Dhurjati (IDIADA) Luca Mengani (IDIADA)	First version of the process and Item Definition	Draft
0.2	27/09/2018	Prashanth Dhurjati (IDIADA)	Updated after comments from project leader	Draft
0.3	29/09/2018	Prashanth Dhurjati (IDIADA) Luca Mengani (IDIADA)	Updated after comments from Work Package leader	Final
1.0	30/09/3029	Prashanth Dhurjati (IDIADA) Luca Mengani (IDIADA)	Ready for submission to EC	Final

FIGURES

EXECUTIVE SUMMARY

CONTEXT AND NEED OF A MULTI BRAND PLATOONING PROJECT

Context

Platooning technology has made significant advances in the last decade, but to achieve the next step towards deployment of truck platooning, an integral multi-brand approach is required. Aiming for Europe-wide deployment of platooning, 'multi-brand' solutions are paramount. It is the ambition of ENSEMBLE to realise pre-standards for interoperability between trucks, platoons and logistics solution providers, to speed up actual market pick-up of (sub)system development and implementation and to enable harmonisation of legal frameworks in the member states.

Project scope

The main goal of the ENSEMBLE project is to pave the way for the adoption of multi-brand truck platooning in Europe to improve fuel economy, traffic safety and throughput. This will be demonstrated by driving up to seven differently branded trucks in one (or more) platoon(s) under real world traffic conditions across national borders. During the years, the project goals are:

- Year 1: setting the specifications and developing a reference design with acceptance criteria
- Year 2: implementing this reference design on the OEM own trucks as well as perform impact assessments with several criteria
- Year 3: focus on testing the multi-brand platoons on test tracks and international public roads

The technical results will be evaluated against the initial requirements. Also, the impact on fuel consumption, drivers and other road users will be established. In the end, all activities within the project aim to accelerate the deployment of multi-brand truck platooning in Europe.

Abstract of this Deliverable

This deliverable consists of 2 parts:

- Iterative development process: As opposed to the classic development process which is linear and pushes risk forward in time, an iterative development process will be defined for this project, so that risks can be identified earlier in development before it is too late and costly to make corrections/changes if required.
- Item Definition: The item definition will define the purpose and describes the functionality of the platooning function, including its various operating modes and states. Common item architecture that shall be used as the reference for all the subsequent safety activities will be defined. The item definition will also compile information on operational and environmental constraints and other legal requirements if applicable.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Background

The purpose of this deliverable is to define an iterative safety work process that can be used throughout the ENSEMBLE project to identify safety risks at an early stage in the development lifecycle so as to give the developers enough time to derive safety mechanisms, implement and test them without incurring delays or adding extra cost to the project.

Classic development processes follow a lifecycle where development approaches proceed linearly from requirement analysis. The fundamental problem of linear approaches is that it pushes risk forward in time so that it's costly to undo mistakes from earlier phases. An initial design will likely be flawed with respect to its key requirements, and, furthermore, the late discovery of design defects tends to result in costly overruns and project cancellations. The approach tends to mask the real risks to a project until it is too late to do anything meaningful about them. Early in the process, it is usually difficult to evaluate different concepts accurately enough for the best solution to be selected. Therefore, an iterative system and safety development process is highly recommended to be used for development of safety critical systems.

This document also provides the details of the feature under development through the "Item definition" work product. The "*Item definition*" defines the purpose and describes the functionality of the platooning function, including its various operating modes and states. This common item architecture will be used as reference for all the subsequent safety activities in the project. The item definition will also compile information on operational and environmental constraints and other legal requirements if applicable.

Since the specification of common solution is still under development, the Item Definition provided in this first version of the deliverable will need further revisions to reflect the final agreement on the system's behaviour. These will be described in the deliverable D 2.11.

Structure of this report

This deliverable is divided into two main sub-sections:

1. Iterative Development Process

2. Item Definition

2. ITERATIVE DEVELOPMENT PROCESS

2.1. Scope of the process

This document describes the process that will be followed to carry out the safety activities at the concept phase and the vehicle integration and testing phase of the development. The development phases are akin to the ones defined in the ISO 26262 standard: Road Vehicles – Functional Safety.

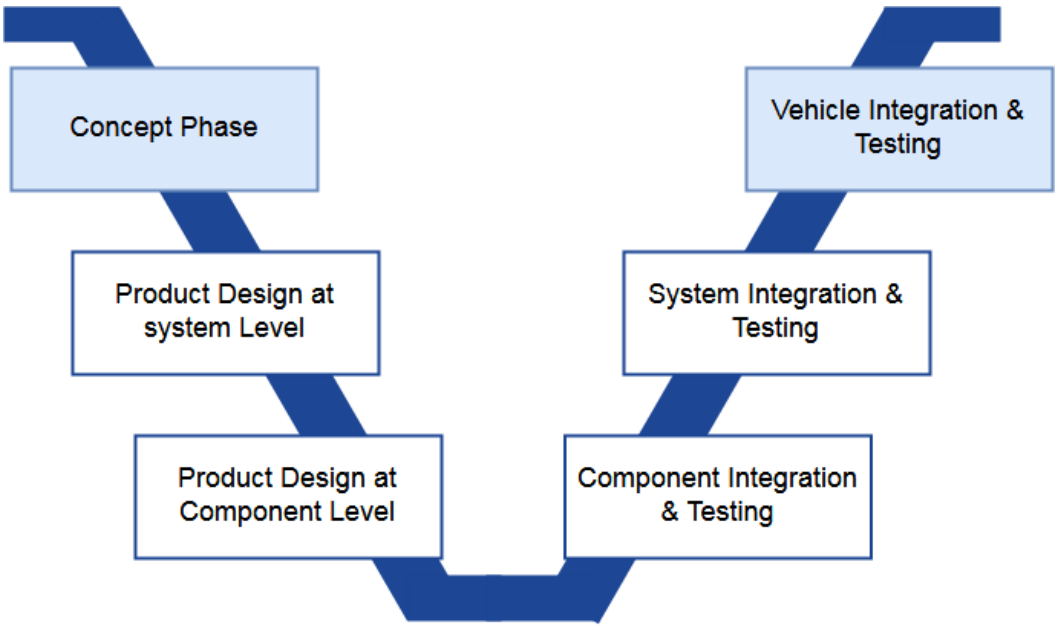

Figure 1 - V Model for Development

The process is described by defining various safety activities that will be carried out at the vehicle level during the project and specify a workflow amongst the activities of each phase.

2.2. The concept phase

As per the ISO 26262 part 3, in concept phase the safety activities are performed on the 'Item'; which is an array of systems that implement a function at the vehicle level'.

The safety activities that will be carried out at the concept phase can be divided into two main categories:

1. Functional Safety: Functional safety seeks to ensure absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems.

   E.g.: Missing V2V messages, Excessive drive torque (unintended acceleration), Insufficient braking, HMI: Lack of information on platoon decoupling, etc.

2. Safety of the Intended Functionality (SOTIF): SOTIF seeks to ensure absence of unreasonable risk due to performance limitations or insufficiencies of the function itself. SOTIF does not deal risks arising from failures of the E/E components.

   E.g.: Emergency braking of the forward vehicle, driving in bad weather conditions, driving on slopes, handling cut-ins at high speed, etc.

2.2.1 The concept phase workflow

The following schematic (Figure 2) outlines the workflow for the activities that will be carried out for both “functional Safety” and “SOTIF” during the concept phase of the project.

Note: In the below schematic, each activity has been assigned a number which references to the description provided in the section 2.2.1.1.

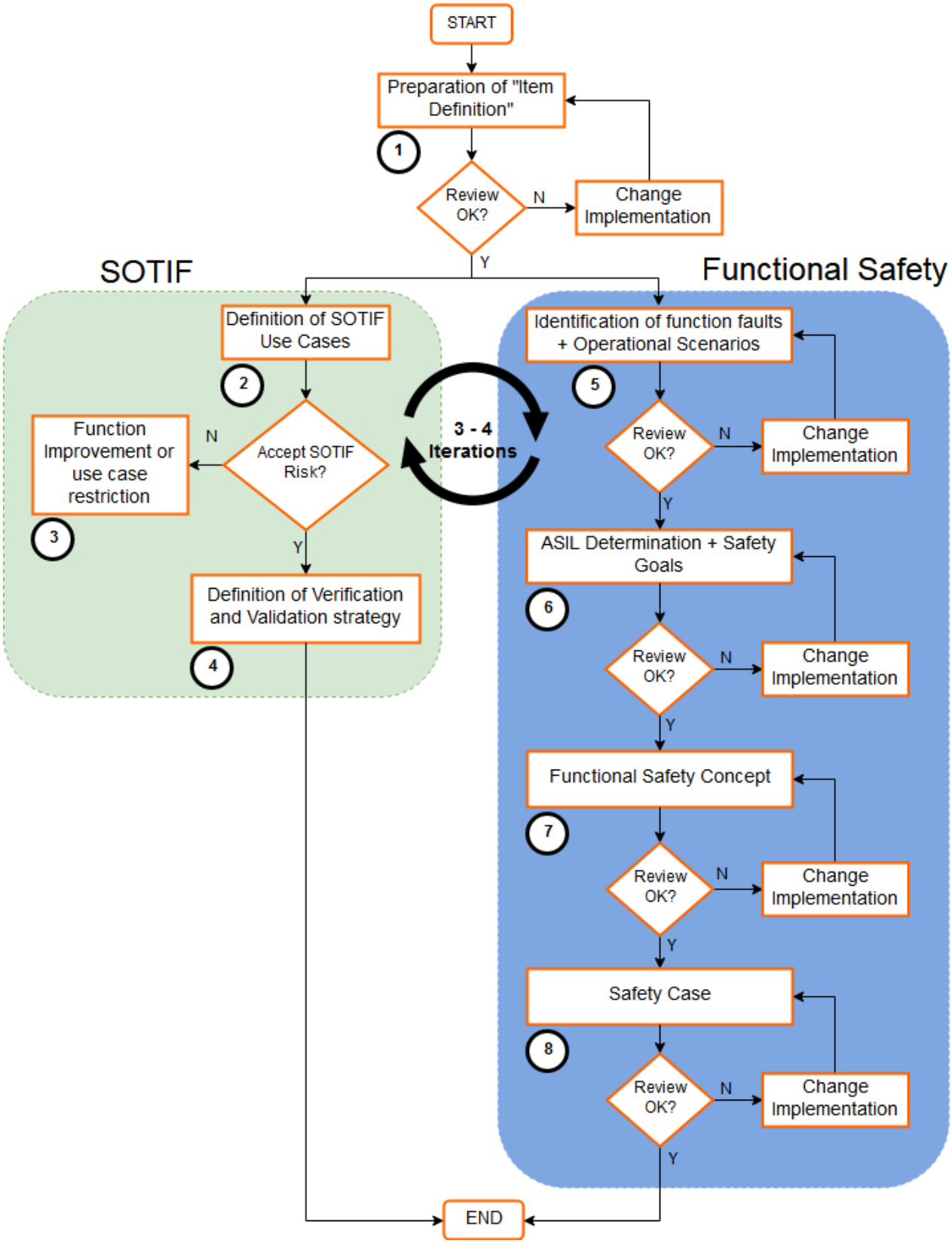

Figure 2 - Workflow concept phase safety activities

Iterative Process for the concept phase

The Safety process for the concept phase shall be iterative in nature. I.e. each of the SOTIF and Functional Safety work products shall undergo multiple loops of definition and reviews before the final version is agreed by the consortium. All the safety work products will be kept alive till the end of the project so that feedback from the implementation and testing phases can be used to modify the existing safety requirements or introduce new ones.

2.2.1.1 Activities common for both SOTIF and Functional Safety:

Review process

As shown in the figure 2, the review process is quite similar for all the work products generated by each activity. Once a work product is complete, it is uploaded to the project share folder for review where the reviewers have around 1 week to evaluate the contents of the item under review and provide feedback. If required, the author can arrange for a call conference to discuss some of the points in detail (e.g. contradicting feedback from different partners) before making the changes and finalizing the work product.

1. **Preparation of Item Definition:**

The first activity of the concept phase which is common for both functional Safety and SOTIF is the preparation of the “Item Definition” work product. The “Item Definition” compiles information on the function under development and is used as the starting point for the safety analysis (both SOTIF and Functional Safety).

The Item definition usually consists of:

- A description of the function that shall be implemented at the vehicle level
- Item boundaries diagram and the function block diagram
- Operational and environmental constraints
- Legal and normative requirements
- Potential consequences of behaviour shortfalls including known failure modes and hazards

2.2.1.2 Activities for SOTIF

2. Definition of SOTIF Use Cases

This activity captures the various scenarios and environmental conditions that might be hazardous for the entire platoon or some of its participants, so that the safety risks associated with each use case can be analysed. Each use case shall also propose an expected reaction from the platoon to manoeuvre through the situation safely. Since SOTIF deals with function limitations, no E/E malfunctions are considered in the scenarios.

3. Function improvement or use case restriction

In case a SOTIF use case is assessed to be risky from the safety's point of view, then one of the following 2 actions will be taken:

1. Improve the function/redefine the specifications so that the situation can be handled safely.

OR

2. Redefine the operational boundaries of the function, so that the function will not be used in certain risky conditions.

4. Definition of SOTIF verification and validation strategies

This activity provides inputs to the WP5, so that tests can be planned to verify the mechanisms implemented to handle the risky SOTIF scenarios safely. Even though there will not be any long term field operational tests planned for the project, some verification tests in controlled environments like test tracks will be planned.

2.2.1.3 Activities for Functional Safety

5. Identification of functional faults + Operational Scenarios

The first task in this activity defines the function faults that will be analysed during the hazard analysis and risk assessment activity. It is important to limit the list to just the failure scenario at the function level without defining the source of the failure; E.g. 'Loss of v2v information' instead of 'V2V antenna failure'. HAZOP methodology will be used to identify the malfunctions at the vehicle level. I.e. focus on the actuators of the item and apply guidewords to postulate malfunctioning behaviours.

Later, the operational scenarios in which the functional faults are to be analysed are defined. These scenarios shall be a combination of the below three factors:

a. What is the vehicle is doing (e.g. accelerating to form a platoon)?

b. Where is the scenario happening (on a highway in rainy conditions)? and

c. What is the situation around the vehicle(s) (other vehicle of the platoon, other road vehicles, construction zone, etc...)?

6. ASIL determination + Safety goals

This activity shall apply automotive specific risk based approach defined in the ISO 26262 to determine the Automotive Safety Integrity Levels (ASILs) for the hazards identified in the previous activity.

The first task in this activity is to determine the risk parameters (Severity, Exposure and Controllability) for each of the hazardous events identified in the previous activity. Once the risk parameters are determined, Automotive Safety Integrity Levels (ASILs) will be assigned to the hazardous event from the standardized matrix provided in the ISO 26262 standard.

Note: Four ASILs are defined in ISO 26262: ASIL A, ASIL B, ASIL C and ASIL D, where ASIL A is the lowest safety integrity level and ASIL D the highest one.

Then safety goals shall be defined for the hazards that have an ASIL greater than 'A' (Lowest safety integrity level). Safety goals are top level safety requirements than are not expressed in terms of technological solutions, but in terms of functional objectives.

7. Definition of the Functional Safety Concept

This activity shall derive the functional safety requirements from the safety goals and allocate them to the E/E functions, other technologies (e.g. mechanical, pneumatic,) and external measures (elements outside the item boundary, e.g. guide rails).

These are implementation independent requirements to the behaviour of the item aimed at achieving the safety goals defined in the previous activity. The functional safety requirements shall be specified by considering, if applicable; the operating modes, the fault tolerant time intervals, safe states, and emergency operational interval and function redundancies.

8. Preparation of the Safety Case

A safety case shall be developed in order to provide an argument for the achievement of functional safety. The safety case shall progressively compile the safety work products that are generated during the project to support the safety argument. Since each OEM might full fill the same safety requirements with different implementations, further discussions are required on how to split the safety case after the concept phase.

The safety case shall be completed by providing evidence from the entire development lifecycle including testing.

2.3. The vehicle integration and testing phase

Once each OEM has completed their integration and testing activities at the system level, the activity of vehicle level integration and testing shall begin. This activity will be carried out in different sub phases as indicated in the below diagram (Figure 3):

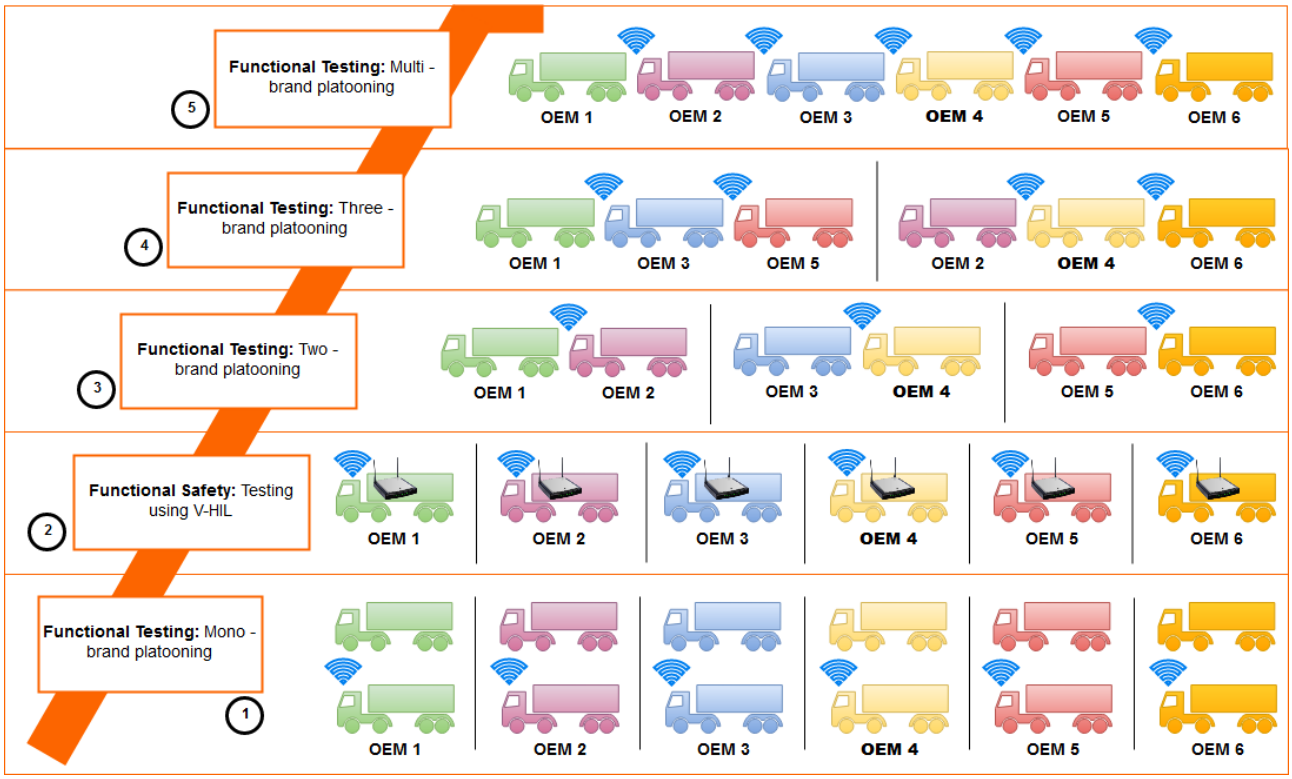

Figure 3 - Vehicle level Integration & Testing

The description of each activity in the above diagram is provided in the section 2.3.1.1.

The test specification, the test setup and the location of each testing activity shall be defined in WP 5.

Iterative Testing Process

The process for the vehicle level integration and testing shall be iterative in nature. I.e. every time a vehicle/OEM fails a test at an integration level and needs to modify its implementation, the previous integration and testing phases have to be repeated to guarantee safety before repeating tests at current level. For e.g. if a vehicle fails a test at two brand platooning level, it has to redo the mono-brand tests and the safety tests before repeating the two brand tests. This regression testing is required to make sure the older implementation is still working as expected after the changes.

2.3.1. Vehicle Integration and Testing workflow

The below workflow diagram outlines the activities that will be carried out at the vehicle level integration and testing phase of the project.

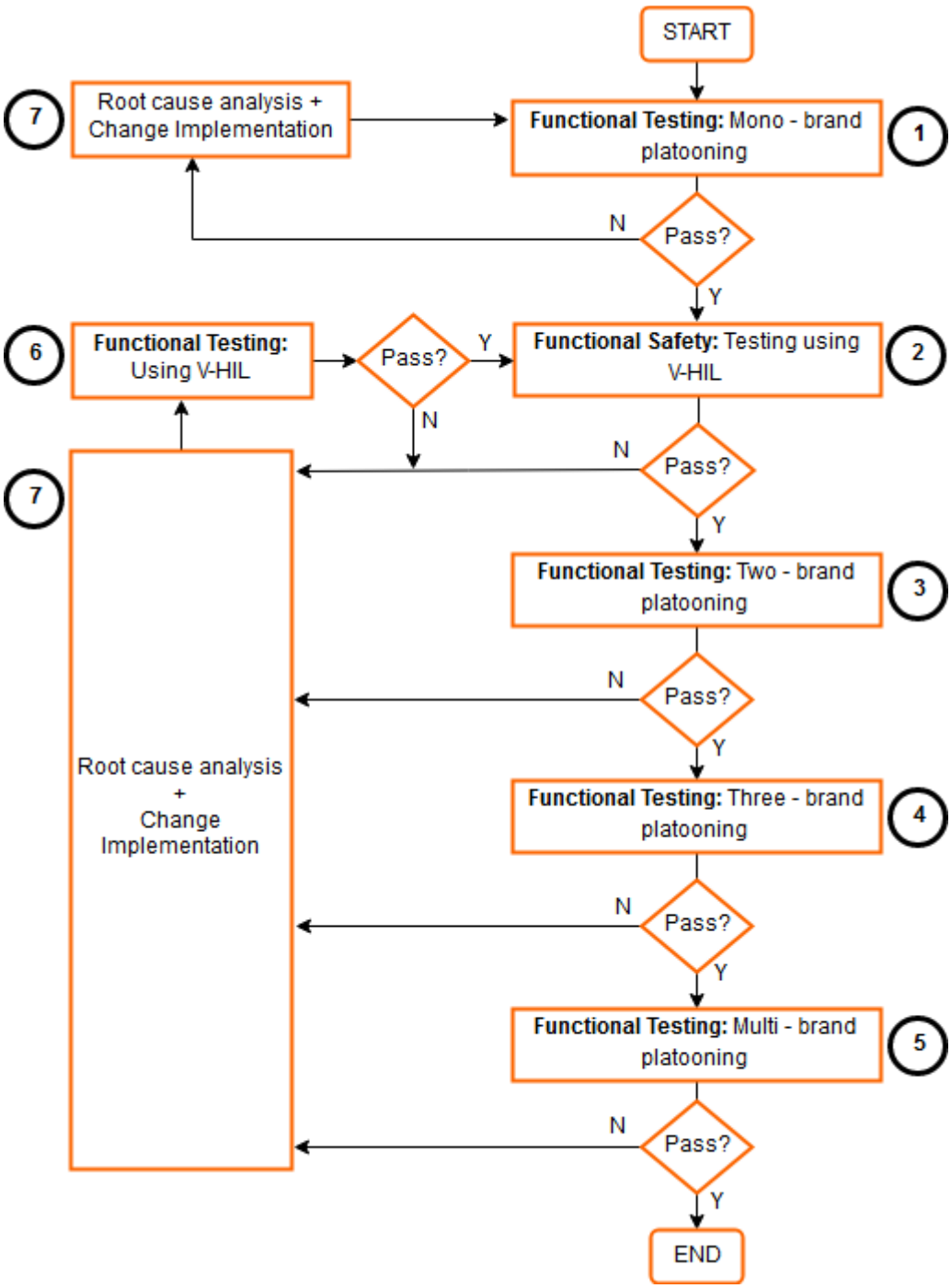

Figure 4 - Workflow Vehicle level integration and testing

Note: In the above schematic, each activity has been assigned a number which references to the description provided in the section 2.3.1.1.

2.3.1.1. Integration and Testing activities

The below section describes the testing activities outlines in the figures 3 and 4:

1. Functional testing – Mono brand platooning:

The first testing activity at the vehicle level shall be the mono brand platooning. Here each OEM shall carry out tests as per the specifications defined in the WP5 using multiple vehicles of their own brand. This step assures that each OEM has correctly integrated their version of the platooning function at the vehicle level.

2. Functional safety testing – V-HIL testing:

The next activity shall be functional safety testing using a V-HIL setup. The V-HIL setup shall allow verification of the functional safety requirements at the vehicle level without compromising the safety of the platoon. The V-HIL setup shall be used to simulate the presence of other vehicles (using multiple V2V communication units) in the platoon and inject faults in the ego vehicle to verify that its safety mechanisms are implemented correctly and the platoon remains safe and controllable under faulty conditions. The test specifications for the functional safety testing shall be defined in WP5.

3. Functional testing – Two brand platooning:

The next activity shall be the functional testing of two brand platooning. Here the OEMs shall form 3 different pairs to carryout functional testing of the platoon as per the test specifications defined in WP5. This activity shall ensure first level of integration with another brand to identify integration errors within different brands.

4. Functional testing – Three brand platooning:

Once the two brands platooning tests are completed with 3 pairs of platoons, functional testing of three brand platooning shall be carried out. Here 2 groups of platoons are formed by putting all the even and odd trucks from the previous group together (Refer to Figure 3 – Vehicle level integration and testing). This step shall ensure interoperability between groups that have not been tested together in the previous integration levels.

5. Functional testing – Multi brand platooning:

The final activity of the testing shall be the functional testing of the multi brand platoon. Here all the vehicles shall be combined together to form a single platoon for the first time and testing activities

shall be carried out as per the specifications defined in the WP5. The test specifications shall also ensure that the roles of lead and following vehicles are taken by all the brands. This step shall ensure the overall integration of all the brands together to form a single platoon.

6. Functional testing – Using V-HIL setup:

If changes are implemented by an OEM as a result of the root cause analysis, then regression testing shall be carried out on the vehicle to ensure safe behaviour of the vehicle before it is again integrated in the platoon with other brands. This can be either done by repeating the mono brand tests before entering into higher levels of integration and testing or by carrying out function tests using the V-HIL setup. The actual procedure shall be defined in the WP5.

The test specifications shall also ensure that the roles of lead and following vehicles are taken by all the brands in the platoon.

7. Root Cause Analysis + Change Implementation

The procedure followed when a test fails shall be common for all the integration levels.

A failed test can be the result of any of the following three reasons:

1. Error in requirements definition
2. Error in implementation
3. Error in test case definition or execution

If a vehicle fails a particular test at any level of integration tests (mono brand, two brand, etc.) an analysis activity shall be carried out by the test team and the OEM to identify the root cause of the failure and if required implement the changes in the system to attain correct results from the tests.

3. ITEM DEFINITION

3.1. Purpose

The purpose of the Item definition document is to support an adequate understanding of the system under development so that the subsequent safety activities can be performed. It should not be considered as a requirements or specifications document for development.

This chapter provides a high-level description of the item as well as the dependencies between the item and its environment. The description includes:

- the functional concept, describing the purpose and functionality, taking into account the operating modes and states of the item;
- the operational constraints;
- the environmental constraints;
- behaviour achieved by similar functions, items or elements, if any;
- assumptions on behaviour expected from the item; and
- potential consequences of behaviour shortfalls including known failure modes and hazards.

Also, the boundary of the item, its interfaces, and the assumptions concerning its interaction with other elements are taken into consideration, considering:

- the elements of the item;
- the assumptions concerning the effects of the item’s behaviour on the vehicles;
- interactions of the item with other elements;
- functionality required by/from other items, elements and the environment;
- the allocation and distribution of functions among the involved elements; and
- the operational scenarios which impact the functionality of the item.

3.2. Item and its elements

The item is an AoS capable of implementing a Platooning level A function at the vehicles level, to which ISO 26262 will be applied.

The multi-brand platooning system consists of elements which also are, in turn, another system. Platooning 'level A' function is distributed among all the involved systems.

Figure 5 shows the item, its elements and the relationship between external elements.

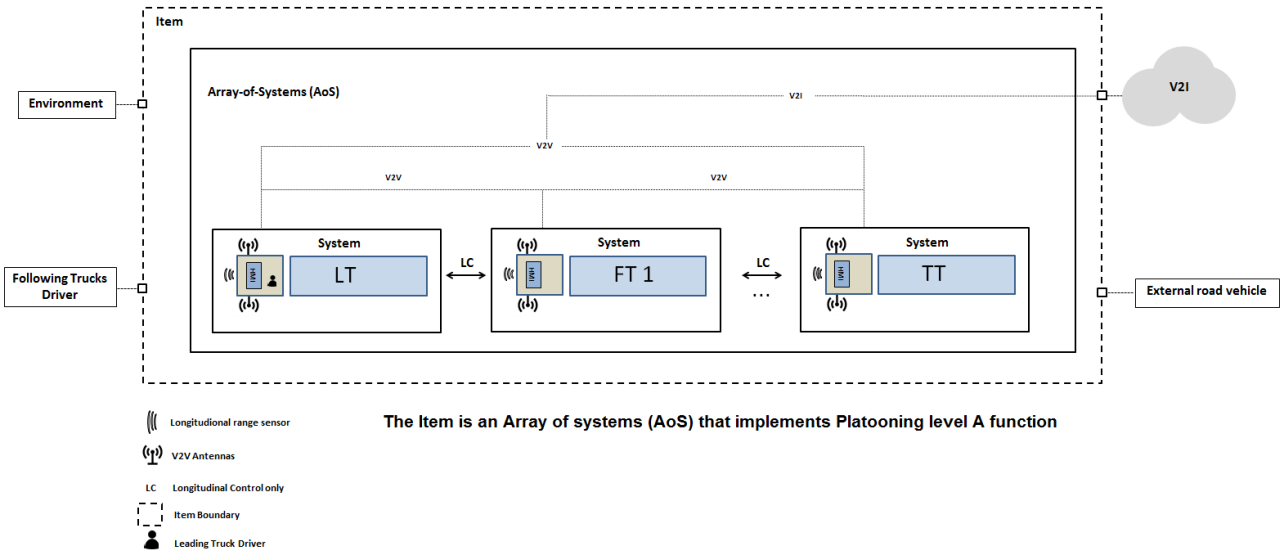

Figure 5 - Item Boundary Diagram

The item consists of the following elements:

- Leading Truck: The LT is the platoon leader. : Longitudinal and lateral vehicle motion controls are not automated by default. Lead vehicle can also be equipped with driver assistance systems (e.g. ACC, LKA). In case the lead vehicle is equipped with ACC, then the longitudinal vehicle motion control can be automated.
- Following Trucks: FTs are the trucks following the lead Truck. In the FTs, the longitudinal vehicle motion control is automated by the platooning function. Following vehicles can also be equipped with driver assistance systems (e.g. LKA).
- Trailing Truck: The last truck in the platoon is called the following truck.
- V2V inter-vehicle communication: vehicles communicate with each other exchanging information such as vehicle position, speed, heading, size, longitudinal acceleration/ deceleration, yaw rate, distance to target ahead, lane marking distance and steering angle.

The item is based on seven multi-brand trucks exchanging data, where six at most are Following Trucks which follow the Lead Vehicle. The trucks take advantages of the mature V2V technology to talk to each other, using DSRC. They are electronically coupled such that acceleration and braking from the Lead Vehicle can nearly simultaneously be initiated by the Following Trucks.

Each vehicle is, in turn, a system which consists of the following components:

- ACC (optional for lead vehicle)
- Forward-looking longitudinal sensor(s)
- GPS system
- Braking system
- Powertrain system
- HMI system

3.2.1. Item Interfaces

The Item boundaries, as shown in Figure 5, are as follows:

- Environment: Driving environment consists of a lot of factors, such as weather and road surface conditions (adverse environmental conditions), road layout (Highway, approaching entry/exit ramp, etc.).
- Leading Truck's Driver: The driver of the lead vehicle remains fully engaged at all times and is responsible for longitudinal and lateral vehicle motion control. In case the lead vehicle is equipped with ACC, then the driver can use it for assistance and be responsible for lateral vehicle motion control, in order to steer. In case the lead vehicle is equipped with LKA, then the driver can use it for assistance. In any case, the driver has the ability to override brake or throttle activation from the system at all times.
- Following Truck driver(s): Following truck driver(s) are only responsible for lateral vehicle motion control, in order to steer, turn, lane keep, lane change and avoid obstacles. In any case, the driver has the ability to override brake or throttle activation from the system at all times.
- Trailing Truck driver: The Trailing truck driver has the same driving responsibilities are that of the other following trucks. Trailing truck can also be equipped with driver assistance systems (e.g. LKA).

- V2I communication: trucks may receive information from infrastructure using several network interfaces (e.g. ITS-G5 or Cellular). The system is expected to receive both tactical and strategic information from infrastructure.

  Tactical information, including:

  a) Restricted Communication Area: there are some areas (e.g. tolling areas) where communication between trucks in the platoon is regulatory based limited;

  b) Platoon Operation Restricted Areas: due to safety, platoon operation might be completely or temporary forbidden/limited in some areas (e.g. tolling, bridges, tunnels, highways with too many exits, rush hour, etc.)

  Strategic information, including:

  a) Billing information;

  b) Remotely scheduled platoon;

  c) Route optimization for platooning

- External Road vehicles performing manoeuvres in real traffic conditions – stop and go, cut-it, cut-out, etc.

3.3. Preliminary functional block diagram

A preliminary functional block diagram is illustrated in the Figure 6, in accordance with the traditional vehicle centric perspective:

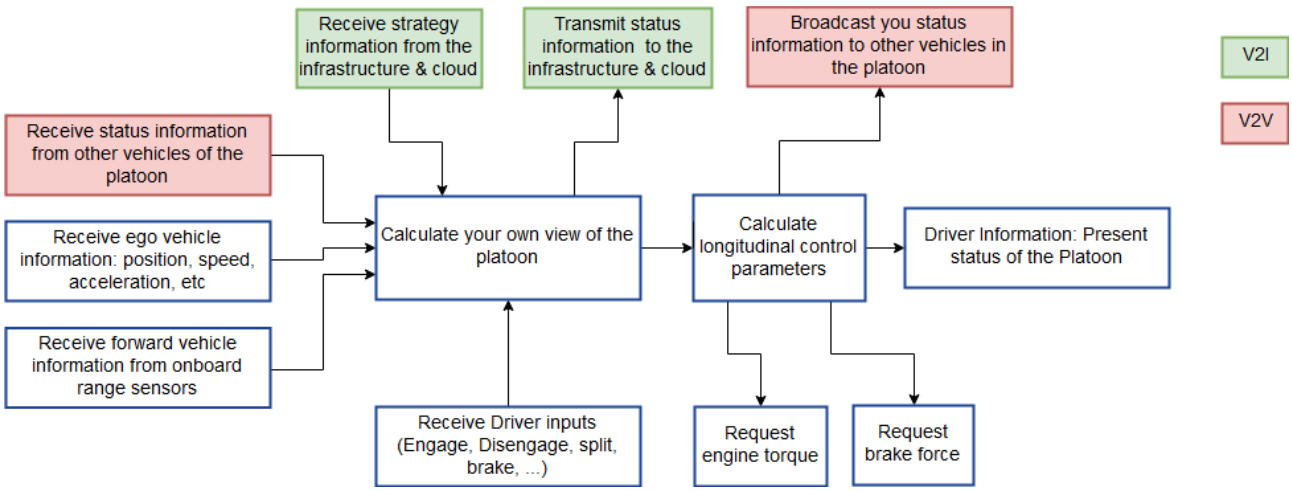

Figure 6 - Function block Diagram

Inputs:

1. The function receives the status information from other vehicles of the platoon via V2V (DSRC) communication.
2. The function receives the ego vehicle information like position, speed, acceleration, etc. from the on board sensors/systems.
3. The function receives information on the forward vehicles like position, speed, acceleration, type, etc. from on board sensors/systems.
4. The function receives driver inputs like platoon engage, platoon disengage, brake, accelerate, etc. from the set point generators.
5. The function receives information from the infrastructure and cloud via Cellular network for platoon formation, weather reports, traffic situation, etc.

Process:

1. The function calculates it's on view of the platoon from the received information.
2. The function calculates parameters for longitudinal control of the ego vehicle in the platoon.

Outputs:

1. The function sends torque request to the powertrain for longitudinal acceleration or deceleration.
2. The function sends deceleration request to the braking system for longitudinal deceleration.
3. The function sends ego vehicle information and status to other vehicles in the platoon via V2V (DSRC) communication.
4. The function sends HMI information to inform the driver about the status of the platoon and other function related parameters.
5. The function sends information to the infrastructure and the cloud via cellular network to provide information on the platoon status, etc.

3.4. Item assumptions

In accordance with the discussions in ENSEMBLE up to now, assumptions on behaviour expected from the item are listed below:

1. Driver of any vehicle can disengage from the platoon at any moment;

2. Engagement will only occur during dynamic driving on the highways;

3. Once established, the platoon is expected to keep cohesion during "stop & go" situations (traffic jams);

4. Administration and road operators may impose operative platoon restrictions. E.g. forbid platoon in some tunnels, increase time gap in bridges, etc.;

5. The maximum number of trucks is up to 7. Actual number on the road may be lower due to authority or road restrictions.

6. New members of a running platoon will always join the platoon from rear.

7. The vehicles shall be able to carry loads as per the legal weight limits of member countries.

8. Under any adverse weather condition, drivers can adjust the time gap or disconnect the platoon under their own criteria (driver education or incentives is out of the scope of the present document);

9. Platoon is expected to be operative in both downhill and uphill. Time gap, speed, and other parameters are expected to be dynamically adapted to ensure platoon cohesion and safety;

10. Platoon is expected to be operative inside tunnels although platoon formation inside the tunnels is excluded.

11. When location information is degraded (e.g. due to poor quality GNSS signal) platooning engagement will not be allowed. If location accuracy is degraded while in an already running platoon, the time gap between trucks is expected to be increased to safe values;

12. Platoon communication will be deactivated when passing toll gates due to ETSI TS 102 792. Deactivation is responsibility of the driver. Platoon might be deactivated automatically based on information received from infrastructure;

13. Each vehicle should be able to maintain safe distance to the forward vehicle, even if V2V information is not available;

14. The project shall aim to attain a time gap of 0.8 seconds for Level A.

3.5. Known failure modes and hazards

- Known failure modes:
  - Malfunction of forward-looking longitudinal sensor;
  - Malfunction of GPS
  - Malfunctions of V2V communication:
    - Delay in communication (excessive latency);
    - Complete loss of communication;
  - Malfunctions of Powertrain:

Provide more drive torque than requested (Unintended acceleration);

Provide less drive torque than requested (Insufficient acceleration);

Loss of torque (loss of acceleration);

- Malfunctions of Braking system:

  Loss of braking,

  Excessive braking when requested;

  Insufficient braking when requested;

  Unintended braking;

  Locked braking;

- Malfunctions of HMI:

  Unintended platoon coupling when not requested;

  Unintended platoon decoupling when not requested;

  Not decoupling when requested (could lead to locked platoon coupling state);

  Lack of information on platoon decoupling;

  Lack of information on platoon coupling;

Other parameters to be considered for safety analysis:

- The environment:
  - Adverse environmental conditions such as bad visibility, wet road, snow and ice on road, slippery road;
  - Road layout such as downhill and entry/exit ramp (e.g. a platoon can obscure road signs from drivers in the outside lanes and potentially make access to entries or exits difficult); unexpected objects on the road ahead or shoulder.
- External Road vehicles, performing manoeuvres like emergency braking, steering, cut-in, cut-through or cut-out.
- Lead and Following driver(s):

- human error due to:
    - looks improperly or wrong judgment of nearby road users speed or path;
    - platooning misuse;
    - lack of driver experience in platooning application
- human manoeuvres caused by the driver, e.g.:
    - emergency braking until vehicle reaches full stop
    - emergency braking aborted before reaching full stop
    - steering in case of unexpected object on the road ahead or shoulder

• V2I, continuous disconnection between a system (truck) and the V2C infrastructure

4. SUMMARY AND CONCLUSION

This report defines the process to be followed to assure the safety of the platooning function being developed in this project and also provides an overview of the Platooning 'level A' feature in the form of 'Item Definition'. The 'Item Definition' describes the platooning function and its dependencies and interactions with other functions of the vehicle and the environment.

4.1. Safety Development process

The safety development process to be used in this project will be iterative in nature, i.e. all the work products will undergo multiple loops of reviews and rework before being finalized.

The safety activities have also been divided into two categories:

1. Functional Safety: Functional safety seeks to ensure absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems.
   E.g.: Missing V2V messages, Excessive drive torque (unintended acceleration), Insufficient braking, HMI: Lack of information on platoon decoupling, etc.

2. Safety of the Intended Functionality (SOTIF): SOTIF seeks to ensure absence of unreasonable risk due to performance limitations or insufficiencies of the function itself. SOTIF does not deal risks arising from failures of the E/E components.
   E.g.: Emergency braking of the forward vehicle, driving in bad weather conditions, driving on slopes, handling cut-ins at high speed, etc.

Safety requirements from both these categories will be derived and implemented for the project.

4.2. Item Definition

At the top level, for the 'level A' feature, each vehicle in the platoon will combine the V2V information received from the forward vehicle in the platoon, the measurement data coming from the forward looking range sensors and the ego vehicle information coming from the in-vehicle sensors to calculate its own view of the platoon. This information is then used to control the longitudinal movement of the vehicle to maintain its position in the platoon in a safe manner.

Some of the main aspects of the 'level A' platooning function are as stated below:

- Maximum number of trucks for safety analysis is limited to 7.
- A time gap of 0.8 seconds will be targeted for the project.
- New members of a running platoon can only join from the rear.
- Platoon engagement can only occur during dynamic driving situations on the highways
- Under adverse conditions like bad weather, slopes, etc.… the drivers have the responsibility to increase the time gap or disengage the platoon completely.

BIBLIOGRAPHY

ISO 26262:2016 (E) – Road Vehicles – Functional Safety

ISO/PRF PAS 21448: Road Vehicles – Safety of the intended functionality

Bosch Case study: Application of SOTIF for ADAS (DR. SUSANNE EBEL, Robert Bosch GmbH)

Josef Nilson, Carl Bergenhem, Rolf Johansson, Jonny Vinter (2013). Functional Safety of Cooperative Systems. SAE Technical Paper. DOI: 10.4271/2013-01-0197

GLOSSARY

Definitions

Term	Definition	Source
Platoon	A group of two or more automated cooperative vehicles in line, maintaining a close distance, typically such a distance to reduce fuel consumption by air drag, increase traffic safety by use of additional ADAS-technology, and improve traffic throughput because vehicles are driving closer together and taking up less space on the road.	
Platoon Level		
Requirement	Statement on what a system should achieve, should be able to perform.	Kick-off meeting
Specifications	Description of system properties. Details of how the requirements shall be implemented at system level	Kick-off meeting / IDIADA
Convoy	A group of two or more vehicles driving together in the same direction, not necessarily at short inter-vehicle distances and not necessarily using advanced driver assistance systems	
Truck Platoon	A truck platoon may be defined as trucks that travel together in convoy formation at a fixed gap distance typically less than 1 second apart up to 0.3 seconds. The vehicles closely follow each other using wireless vehicle-to-vehicle (V2V) communication and advanced driver assistance systems	Adapted from ACEA website
Leading Truck	The first vehicle of the platoon, which takes the role of the platoon leader.	Use case meetings
Following Truck(s)	All the tracks following the leading truck except the last truck in the platoon. There can be more than one following trucks e.g. FT1, FT2, etc.	Use case meetings

Trailing Truck	The last truck of the platoon.	Use case meetings

Acronyms and abbreviations

Acronym / abbreviation	**Meaning**
ACC	Adaptive Cruise Control
ADAS	Advanced driver assistance system
AEB	Autonomous Emergency Braking (System, AEBS)
AoS	Array of Systems
ASIL	Automotive Safety Integrity Level
ASN.1	Abstract Syntax Notation One
BTP	Basic Transport Protocol
C-ACC	Cooperative Adaptive Cruise Control
C-ITS	Cooperative ITS
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
CCH	Control Channel
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short-Range Communications
ETSI	European Telecommunications Standards Institute
EU	European Union

FCW	Forward Collision Warning
FLC	Forward Looking Camera
FSC	Functional Safety Concept
FuSa	Functional Safety
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability study
HIL	Hardware-in-the-Loop
HMI	Human Machine Interface
HW	Hardware
I/O	Input / Output
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITS	Intelligent Transport System
LDWS	Lane Departure Warning System
LKA	Lane Keeping Assist
LCA	Lane Centering Assist
LRR	Long Range Radar
MRR	Mid Range Radar
OS	Operating system
ODD	Operational Design Domain
PAEB	Platooning Autonomous Emergency Braking

PMC	Platooning Mode Control
RSU	Road Side Unit
SAE	SAE International, formerly the Society of Automotive Engineers
SCH	Service Channel
SDO	Standard Developing Organisations
SIL	Software-in-the-Loop
SOTIF	Safety of the Intended Functionality
SRR	Short Range Radar
V-HIL	Vehicle – Hardware In the Loop Simulator
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to any (where x equals either vehicle or infrastructure)
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)
WIFI	Wireless Fidelity
WP	Work Package